Radio-relay apparatus for cable television system, has modem which registers media access control address from radio terminal side, when modem is not connected to transmission line
Patent Assignee: MASPRO DENKO KK
Inventors: SATAKE M; SHINODA M

Patent Family (1 patent, 1 country)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 2003110570	A	20030411	JP 2001301507	A	20010928	200352	B

Priority Application Number (Number Kind Date): JP 2001301507 A 20010928

Patent Details

Patent Number	Kind	Language	Pages	Drawings	Filing Notes
JP 2003110570	A	JA	11	8	

Alerting Abstract: JP A

NOVELTY - A radio cable modem (20) connected to transmission line (6) of CATV system, relays data communication between radio terminals (12-16) and center apparatus (2). The modem registers media access control (MAC) address from radio terminal side, when modem is not connected to the transmission line. When modem is connected to transmission line, the access from radio terminal with non-registered MAC address is refused.

DESCRIPTION - An INDEPENDENT CLAIM is also included for bidirectional CATV system.

USE - Radio-relay apparatus connected with local area network for bidirectional cable television (CATV) system.

ADVANTAGE - Reliably prevents the unauthorized access to the apparatus by registering the unauthorized-access prevention parameters.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of a bidirectional CATV system. (Drawing includes non-English language text).

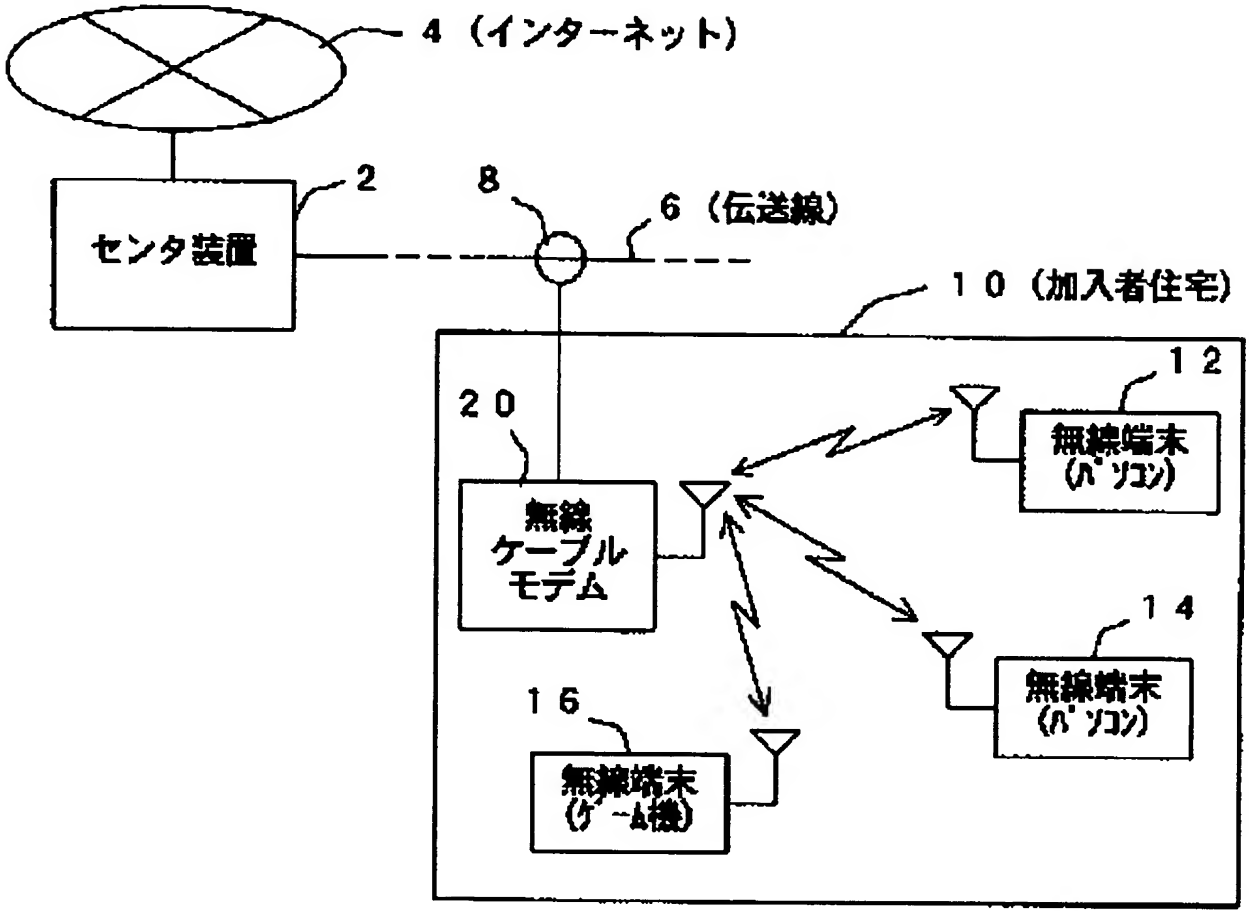
2 center apparatus

6 transmission line

12-16 radio terminals

20 cable modem

Main Drawing Sheet(s) or Clipped Structure(s)



International Classification (Main): H04L-012/28 **(Additional/Secondary):** H04B-007/15, H04B-007/26, H04L-012/46, H04Q-007/38

Original Publication Data by Authority

Japan
Publication Number: JP 2003110570 A (Update 200352 B)
Publication Date: 20030411
WIRELESS REPEATER AND TWO-WAY CATV SYSTEM
Assignee: MASPRO DENKOH CORP (MSPU)
Inventor: SATAKE MASAYUKI SHINODA MITSUO
Language: JA (11 pages, 8 drawings)
Application: JP 2001301507 A 20010928 (Local application)
Original IPC: H04L-12/28(A) H04B-7/15(B) H04B-7/26(B) H04L-12/46(B) H04Q-7/38(B)
Current IPC: H04L-12/28(A) H04B-7/15(B) H04B-7/26(B) H04L-12/46(B) H04Q-7/38(B)

Derwent World Patents Index

Dialog® File Number 351 Accession Number 13455108

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－110570
（P2003－110570A）
(43)公開日　平成15年４月11日(2003.4.11)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/28	３００	Ｈ０４Ｌ　12/28	３００Ａ	５Ｋ０３３
Ｈ０４Ｂ　7/15		12/46	Ｚ	５Ｋ０６７
7/26		Ｈ０４Ｂ　7/26	Ａ	５Ｋ０７２
Ｈ０４Ｌ　12/46		7/15	Ｚ	
Ｈ０４Ｑ　7/38		7/26	１０９Ｒ	

審査請求　未請求　請求項の数８　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－301507(P2001－301507)

(22)出願日　平成13年９月28日(2001.9.28)

(71)出願人　000113665
マスプロ電工株式会社
愛知県日進市浅田町上納80番地

(72)発明者　佐竹　正行
愛知県日進市浅田町上納80番地　マスプロ電工株式会社内

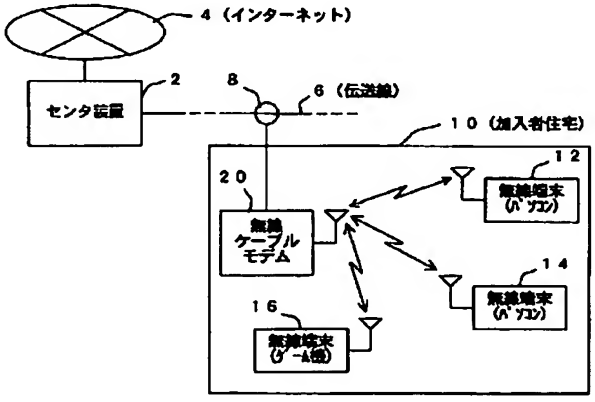
(72)発明者　篠田　光生
愛知県日進市浅田町上納80番地　マスプロ電工株式会社内

(74)代理人　100082500
弁理士　足立　勉

最終頁に続く

(54)【発明の名称】　無線中継装置及び双方向ＣＡＴＶシステム

(57)【要約】
【課題】　無線端末と伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置において、無線端末を利用した第三者の不正アクセスを確実に防止し、不正アクセス防止用のパラメータを安全に登録できるようにする。
【解決手段】　双方向ＣＡＴＶシステムの伝送線６に接続された無線ケーブルモデム２０は、加入者の無線端末１２～１６との間で無線通信を行うことにより、各無線端末１２～１６とセンタ装置２との間のデータ通信を中継する。無線ケーブルモデム２０は、伝送線６に接続されていないときに、無線端末側からＭＡＣアドレスを登録できるようになっており、伝送線６に接続されると、ＭＡＣアドレスが登録されていない無線端末からのアクセスを拒否する。また、無線端末のＭＡＣアドレスが何も登録されていないときには、全ての無線端末からのアクセスを拒否する。



1

【特許請求の範囲】

【請求項１】　データ伝送可能な伝送線に接続され、該伝送線に接続されない無線端末との間で無線通信を行うことにより、該無線端末と前記伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置であって、

前記データ通信の中継を行う無線端末を制限するための制限情報を記憶する記憶手段と、

該記憶手段に記憶された制限情報に基づき、前記データ通信の中継を行う無線端末を制限する無線端末制限手段と、

前記無線端末から無線にて送信されてくる登録要求に従い、前記無線端末と無線通信することにより、前記無線端末から前記制限情報を取得し、該制限情報を前記記憶手段に登録する制限情報登録手段と、

を備え、

前記無線端末制限手段は、前記記憶手段に前記制限情報が登録されていない場合に、全ての無線端末に対して、前記データ通信の中継を禁止し、

前記制限情報登録手段は、当該装置の使用者により前記制限情報の登録が許可されている場合に、前記無線端末からの登録要求を受け付け、前記制限情報の登録が許可されていない場合には、前記無線端末からの登録要求を拒否することを特徴とする無線中継装置。

【請求項２】　前記制限情報登録手段は、当該無線中継装置が前記伝送線に接続されていないときに、前記制限情報の登録が許可されていると判断して、前記無線端末からの登録要求を受け付け、当該無線中継装置が前記伝送線に接続されているときには、前記制限情報の登録が許可されていないと判断して、前記無線端末からの登録要求を拒否することを特徴とする請求項１記載の無線中継装置。

【請求項３】　前記制限情報は、少なくとも、前記データ通信の中継を許可された無線端末のＭＡＣアドレスを含み、

前記無線端末制限手段は、前記記憶手段に前記ＭＡＣアドレスが登録されている際には、当該無線中継装置にアクセスしてきた無線端末のＭＡＣアドレスが前記記憶手段に登録されているか否かを判断して、登録されている場合に、該無線端末と前記通信装置との間のデータ通信の中継を許可することを特徴とする請求項１又は請求項２に記載の無線中継装置。

【請求項４】　前記制限情報は、少なくとも、前記データ通信の中継を許可された無線端末が属するグループを表すグループ情報を含み、

前記無線端末制限手段は、前記記憶手段に前記グループ情報が登録されている際には、当該無線中継装置にアクセスしてきた無線端末が前記記憶手段に登録されたグループに属するか否かを判断して、該無線端末が該グループに属する場合に、該無線端末と前記通信装置との間のデータ通信の中継を許可することを特徴とする請求項１～請求項３何れか記載の無線中継装置。

2

【請求項５】　前記制限情報は、少なくとも、前記データ通信の中継を許可された無線端末との間の無線通信を暗号化して行うため暗号鍵を含み、

前記無線端末制限手段は、

前記記憶手段に前記暗号鍵が登録されている場合に、前記無線端末から送信されてきたデータを前記暗号鍵を用いて復号化し、前記無線端末へ送信するデータを前記暗号鍵を用いて暗号化することにより、前記通信装置との間のデータ通信が可能な無線端末を制限する暗号処理手段、

を備えたことを特徴とする請求項１～請求項４何れか記載の無線中継装置。

【請求項６】　前記無線端末制限手段は、前記記憶手段に前記制限情報が登録されていない場合に、当該無線中継装置にアクセスしてきた無線端末のＭＡＣアドレスからベンダーＩＤを読み出し、該ベンダーＩＤが当該無線中継装置に付与されたＭＡＣアドレスと同じベンダーＩＤであれば、該無線端末と前記通信装置との間のデータ通信の中継を許可し、該ベンダーＩＤが異なっていれば、該無線端末と前記通信装置との間のデータ通信の中継を禁止することを特徴とする請求項１～請求項５何れか記載の無線中継装置。

【請求項７】　前記無線中継装置は、双方向ＣＡＴＶシステムの伝送線の加入者側末端部に接続され、加入者側無線端末との間で無線通信を行うことで、加入者側無線端末と双方向ＣＡＴＶシステムのセンタ装置との間のデータ通信を中継する無線ケーブルモデムであることを特徴とする請求項１～請求項６何れか記載の無線中継装置。

【請求項８】　テレビ放送信号伝送用の伝送線を介してセンタ装置と加入者側端末との間でデータ通信が可能な双方向ＣＡＴＶシステムにおいて、

前記伝送線の加入者側末端部に、加入者側無線端末との間で無線通信を行う無線ケーブルモデムとして、請求項７記載の無線中継装置を備えたことを特徴とする双方向ＣＡＴＶシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ伝送可能な伝送線に接続され、この伝送線に接続されない無線端末との間で無線通信を行うことにより、無線端末と伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置に関する。

【０００２】

【従来の技術】従来より、この種の無線中継装置として、例えば、有線ＬＡＮ（local area network）の伝送線に接続されて、無線端末との間で無線通信を行う無線基地局、或いは、インターネット接続サービスを行う双

方向ＣＡＴＶシステムの伝送線に接続されて、ＣＡＴＶシステムの加入者側無線端末との間で無線通信を行う無線ケーブルモデム、等が知られている。

【０００３】ところで、この種の無線中継装置では、通常、無線端末との間で、米国電気電子学会の無線ＬＡＮの仕様（例えば、「ＩＥＥＥ８０２．１１ｂ」）に準拠したプロトコルで無線通信を行うように構成されていることから、ＬＡＮ若しくはＣＡＴＶシステムに加入していないものが、上記規格に準拠した汎用の無線端末を使って、無線中継装置にアクセスできる。

【０００４】このため、上記無線中継装置には、アクセスが許可された無線端末のＭＡＣアドレス（Media Access Control adress ）やＳＳＩＤ（Service Set Identification）を登録することにより、アクセス可能な無線端末を制限したり、或いは、予め無線端末と共通の暗号鍵を登録しておき、無線端末との間でその共通の暗号鍵を利用して暗号化データを送受信することにより、無線中継装置への不正アクセスを防止することが行われている。

【０００５】尚、ＭＡＣアドレスは、ネットワークでホストを識別するために設定されるハードウェア固有のアドレスである。そして、このＭＡＣアドレスを利用すれば、例えば、アクセスが許可された無線端末のＭＡＣアドレスを無線中継装置に予め登録しておくことにより、その登録した無線端末以外のものから無線中継装置へのアクセスを制限する、といったことができる。

【０００６】また、ＳＳＩＤは、通信相手を特定するための識別番号であり、このＳＳＩＤが同じ装置同士でのみ、無線通信を可能とするものである。従って、ＳＳＩＤを利用すれば、例えば、アクセスが許可された無線端末と同じＳＳＩＤを無線中継装置に予め登録しておくことによって、その登録したＳＳＩＤが付与されていない無線端末から無線中継装置へのアクセスを制限する、といったことができる。

【０００７】また、無線中継装置と無線端末との間で暗号化データを送受信する際には、一般に、ワイヤレスネットワークのセキュリティを確保するためのプロトコルであるＷＥＰ（Wired Equivalent Privacy）が利用される。そして、このＷＥＰを利用すれば、無線中継装置と無線端末との間で暗号化データが送受信されることから、無線中継装置と同じ暗号鍵を有する無線端末のみが無線中継装置にアクセスすることができるようになり、無線中継装置に不正にアクセスしてきた無線端末は無線中継装置に認識されず、他の通信装置とデータ通信ができなくなる。

【０００８】

【発明が解決しようとする課題】このように従来の無線中継装置は、ＭＡＣアドレス、ＳＳＩＤ、ＷＥＰ等を利用して、アクセス可能な無線端末を制限できるように構成されているのであるが、従来の無線中継装置は、通常、これらアクセス制限用のパラメータ（ＭＡＣアドレス、ＳＳＩＤ、ＷＥＰ用の暗号鍵）を使用者が設定しなければ、無線中継装置と同じ仕様（例えば「ＩＥＥＥ８０２．１１ｂ」）のプロトコルで無線通信を行う無線端末から自由にアクセスできるようになっていた。

【０００９】このため、無線中継装置が接続される有線ＬＡＮや双方向ＣＡＴＶシステムでは、上記のようなアクセス制限用のパラメータを設定していない無線中継装置を介して、第三者による不正侵入が行われることがあった。一方、こうした問題を防止するためには、無線中継装置を、上述した不正アクセスを防止するためのパラメータが設定されていない場合に、全ての無線端末のアクセスを禁止するように構成すればよい。

【００１０】しかしながら、このように上記パラメータが設定されていない場合に、無線端末から無線中継装置へのアクセスを全て禁止すると、無線端末を利用して上記パラメータを設定することができなくなり、使い勝手が悪いという問題が生じる。また、この場合、上記パラメータの設定を、伝送線を介して無線中継装置に接続される通信装置から行うようにすることもできるが、このようにすると、伝送線に接続可能な第三者から上記パラメータが不正に設定される虞がある。

【００１１】これに対して、上記パラメータの設定だけは、無線通信によって無線端末側から行えるようにすることもできるが、無線中継装置をこのように構成すると、今度は、第三者が自分の無線端末を利用できるように上記パラメータを設定することが可能となり、第三者による無線端末を使った不正アクセスを防止することができなくなってしまう。

【００１２】本発明は、こうした問題に鑑みなされたものであり、有線ＬＡＮや双方向ＣＡＴＶシステム等の伝送線に接続されて、無線端末と伝送線に接続された他の通信装置との間のデータ通信を中継する無線中継装置において、無線端末を利用した第三者の不正アクセスを確実に防止でき、しかもその不正アクセス防止用のパラメータを、無線端末を利用して安全に登録できるようにすることを目的とする。

【００１３】

【課題を解決するための手段及び発明の効果】かかる目的を達成するためになされた請求項１に記載の無線中継装置は、データ通信の中継を行う無線端末を制限するための制限情報を記憶する記憶手段を備え、無線端末制限手段が、その記憶手段に記憶された制限情報に基づき、データ通信の中継を行う無線端末を制限し、しかも、記憶手段に制限情報が登録されていない場合には、全ての無線端末に対して、データ通信の中継を禁止する。

【００１４】このため、本発明の無線中継装置を用いれば、記憶手段に記憶された制限情報により制限を受けない無線端末のみが、伝送線に接続された他の通信装置との間のデータ通信が可能となり、第三者が自分の所有す

る無線端末を利用して無線中継装置を不正使用することは不可能になる。

【００１５】一方、記憶手段への制限情報の登録は、無線端末側から登録要求を無線にて送信することにより起動される制限情報登録手段を介して、無線端末側から行うことができる。そして、本発明において、この制限情報登録手段は、使用者により制限情報の登録が許可されている場合にだけ、無線端末からの登録要求を受け付け、制限情報の登録が許可されていない場合には無線端末からの登録要求を拒否するように構成されることから、第三者が自分の無線端末を利用して記憶手段に制限情報を書き込むことはできなくなる。

【００１６】よって、本発明の無線中継装置によれば、無線端末を利用した第三者の不正アクセスを確実に制限でき、しかもその不正アクセス制限用の制限情報を無線端末を利用して安全に登録できることになる。ここで、制限情報登録手段は、使用者により制限情報の登録が許可されている場合にだけ無線端末からの登録要求を受け付けるが、このためには、無線中継装置に、使用者が制限情報の登録を許可するか否かを手動操作で切り替えるための切換スイッチを設けるようにしてもよい。

【００１７】しかし、このような切換スイッチを設けると、制限情報登録後の使用者の操作忘れによって、第三者が自分の無線端末を利用して記憶手段に制限情報を登録できるようになることも考えられるので、より好ましくは、制限情報登録手段を、請求項２に記載のようにするとよい。

【００１８】即ち、請求項２に記載の無線中継装置では、制限情報登録手段は、当該無線中継装置が伝送線に接続されていないときに、制限情報の登録が許可されていると判断して、無線端末からの登録要求を受け付け、当該無線中継装置が伝送線に接続されているときには、制限情報の登録が許可されていないと判断して、無線端末からの登録要求を拒否するように構成される。

【００１９】この結果、請求項２に記載の無線中継装置によれば、無線端末を利用した制限情報の登録は、当該無線中継装置を伝送線に接続する前、若しくは、当該無線中継装置を伝送線から外してから行う必要があり、当該無線中継装置が伝送線に接続されているときには、制限情報の登録を行うことができなくなるので、当該無線中継装置が伝送線に接続されて通常動作状態にあるときには、第三者が自分の無線端末を利用して記憶手段に制限情報を書き込むことはできなくなり、第三者による無線中継装置の不正使用をより確実に防止できる。

【００２０】一方、記憶手段に登録する制限情報としては、請求項３に記載のように、データ通信の中継を許可された無線端末のＭＡＣアドレスであっても、請求項４に記載のように、データ通信の中継を許可された無線端末が属するグループを表すグループ情報（例えば、上述のＳＳＩＤ等）であっても、請求項５に記載のように、

データ通信の中継を許可された無線端末との間の無線通信を暗号化して行うため暗号鍵（例えば、上述のＷＥＰでデータ通信に制限をかけるための暗号鍵）であっても、或いは、これらのパラメータを組み合わせてもよい。

【００２１】そして、ＭＡＣアドレスを制限情報として記憶手段に登録できるように構成した際には、無線端末制限手段を、記憶手段にＭＡＣアドレスが登録されている際に、当該無線中継装置にアクセスしてきた無線端末のＭＡＣアドレスが記憶手段に登録されているか否かを判断して、登録されている場合に、その無線端末と伝送線に接続された通信装置との間のデータ通信の中継を許可するように構成すればよい（請求項３参照）。

【００２２】また、ＳＳＩＤ等のグループ情報を制限情報として記憶手段に登録できるように構成した際には、無線端末制限手段を、記憶手段にグループ情報が登録されている際に、当該無線中継装置にアクセスしてきた無線端末が記憶手段に登録されたグループに属するか否かを判断して、無線端末が記憶手段に登録されたグループに属する場合に、その無線端末と伝送線に接続された通信装置との間のデータ通信の中継を許可するように構成すればよい（請求項４参照）。

【００２３】一方、ＷＥＰ等のプロトコルで利用される暗号鍵を制限情報として記憶手段に登録できるように構成した際には、請求項５に記載のように、無線端末制限手段に暗号処理手段を設けるようにすればよい。つまり、請求項５に記載の無線中継装置において、暗号処理手段は、記憶手段に暗号鍵が登録されている際に、無線端末から送信されてきたデータを、記憶手段に登録された暗号鍵を用いて復号化し、無線端末へ送信するデータを、記憶手段に登録された暗号鍵を用いて暗号化することから、通信装置との間のデータ通信が可能な無線端末は、記憶手段に登録されたものと同じ暗号鍵を用いて送信データの暗号化、受信データの復号化を行う無線端末に制限され、この暗号鍵を用いてデータ通信を行うことのできない無線端末は、無線中継装置を利用したデータ通信を行うことができなくなる。

【００２４】ところで、請求項１～請求項５に記載の無線中継装置において、記憶手段に制限情報（ＭＡＣアドレス、ＳＳＩＤ等のグループ情報、ＷＥＰ等のプロトコルで利用される暗号鍵等）が登録されていなければ、無線端末制限手段は、無線中継装置にアクセスしてきた全ての無線端末に対して、伝送線に接続された他の通信装置との間のデータ通信の中継を禁止するが、このような無線中継装置は、無線端末を操作して無線中継装置に制限情報を登録することができない使用者にとっては極めて使い勝手の悪いものとなってしまう。

【００２５】そこで、本発明（請求項１～請求項５）の無線中継装置においては、無線端末制限手段を、請求項６に記載のように構成してもよい。即ち、請求項６に記

載の無線中継装置において、無線端末制限手段は、記憶手段に制限情報が登録されていない場合に、当該無線中継装置にアクセスしてきた無線端末のＭＡＣアドレスからベンダーＩＤを読み出し、そのベンダーＩＤが当該無線中継装置に付与されたＭＡＣアドレスと同じベンダーＩＤである場合に限って、その無線端末と通信装置との間のデータ通信の中継を許可するように構成してもよい。

【００２６】つまり、ＭＡＣアドレスは、４８ビット（換言すれば６バイト）のデジタルデータからなり、そのうちの前半２４ビットがＩＥＥＥ（米国電気電子学会）で管理された管理組織固有のＩＤ（ベンダーＩＤ）、後半２４ビットが無線端末（若しくはパーソナルコンピュータ等の情報機器を無線端末として利用するために装着されるＮＩＣ（ネットワークインターフェイスカード））固有の番号、となっていることから、請求項６に記載の無線中継装置では、このＭＡＣアドレスを構成しているベンダーＩＤを利用して、無線中継装置を利用可能な無線端末を制限するのである。

【００２７】そして、このようにすれば、無線中継装置の所有者は、無線中継装置を購入する際、無線中継装置とベンダーＩＤが同じ無線端末（若しくはＮＩＣ）を購入すれば、これらをそのまま使って、伝送線上の他の通信装置との間でデータ通信を行うことができることから、無線中継装置の使い勝手を向上できる。

【００２８】尚、この場合、無線中継装置に付与されたＭＡＣアドレスと同じベンダーＩＤのＭＡＣアドレスを有する無線端末（換言すれば、無線中継装置と製造会社が同じ無線端末）については、何ら制限を受けることなく、無線中継装置を利用できることになるが、無線中継装置を不正に利用しようとする第三者は、この無線中継装置と同じ製造会社から供給される無線端末を準備しなければならないため、従来に比べて、無線中継装置の不正使用を防止できる。

【００２９】次に、請求項７に記載の無線中継装置は、上述した本発明（請求項１～請求項６）の無線中継装置を、双方向ＣＡＴＶシステムの伝送線の加入者側末端部に接続されて、加入者側無線端末と双方向ＣＡＴＶシステムのセンタ装置との間のデータ通信を中継する無線ケーブルモデムに適用したものである。

【００３０】そして、このように本発明（請求項１～請求項６）に無線中継装置を双方向ＣＡＴＶシステム用の無線ケーブルモデムに適用した場合、この無線ケーブルモデムを使って、双方向ＣＡＴＶシステムにて提供されるインターネットサービス等のデータ通信サービスを加入者以外の者が不正に利用できるようになるのを防止し、延いては、この不正利用に伴い正規の加入者が不利益を被るのを防止できる。

【００３１】また次に、請求項８に記載の発明は、請求項７に記載の無線中継装置（無線ケーブルモデム）を伝送線の加入者側末端部に備え、無線中継装置（無線ケーブルモデム）を利用して加入者側無線端末とセンタ装置との間のデータ通信を行えるようにした双方向ＣＡＴＶシステムに関するものである。

【００３２】そして、この双方向ＣＡＴＶシステムによれば、双方向ＣＡＴＶシステムが提供するインターネットサービス等のデータ通信サービスを、加入者以外の者が不正に利用するのを防止し、この不正利用に伴い正規の加入者が不利益を被るのを防止できる。

【００３３】

【発明の実施の形態】以下に、本発明の実施例を図面と共に説明する。図１は、本発明が適用された実施例の双方向ＣＡＴＶシステムの概略構成図であり、図２は、この双方向ＣＡＴＶシステムの伝送線６の加入者側末端部に接続された無線ケーブルモデム（本発明の無線中継装置に相当する）の構成を表すブロック図である。

【００３４】図１に示すように、本実施例の双方向ＣＡＴＶシステムは、インターネット４に接続され、加入者側の端末装置（図では、無線端末１２、１４、１６）からの要求に従い、その端末装置をインターネット４に接続するＩＳＰ（インターネットサービスプロバイダ）としての機能を有するセンタ装置２を備える。

【００３５】そして、このセンタ装置２から出力される所定周波数帯（例えば、７０ＭＨｚ～７７０ＭＨｚ）の下り信号（テレビ放送信号やデータ通信用の信号）は伝送線６を介して加入者側の端末装置へと下り方向に伝送され、加入者側の端末装置から出力された所定周波数帯（例えば、５ＭＨｚ～４２ＭＨｚ）の上り信号（データ通信用の信号）は、下り信号と同じ伝送線６を介して、センタ装置２側へと上り方向に伝送される。

【００３６】また、伝送線６には、下り信号及び上り信号を夫々増幅し、必要に応じて伝送線６を分岐する図示しない増幅器や分岐増幅器が複数設けられ、更に、加入者住宅１０の近傍で伝送線６を加入者住宅１０まで引き込むためのタップオフ（分岐器）８も多数設けられている（図ではそのうちの一つを記載）。

【００３７】このため、本実施例の双方向ＣＡＴＶシステムにおいて、インターネット接続サービスに加入している加入者は、タップオフ８や図示しない保安器等を介して加入者住宅１０内に引き込まれた伝送線６の末端部に、有線のケーブルモデム若しくは図１に示す無線ケーブルモデム２０を接続し、更に、このケーブルモデムに、インターネットにアクセス可能な情報端末（パーソナルコンピュータ，ゲーム機等）を有線若しくは無線で接続することにより、この情報端末を使ってインターネットを利用できる。

【００３８】また、伝送線６の末端部に無線ケーブルモデム２０が接続された加入者住宅１０では、情報端末として、無線ＬＡＮの通信機能を有する無線端末、若しくは、無線ＬＡＮ用のＮＩＣ（ＰＣカードやパーソナルコ

ンピュータの拡張ボード）をパーソナルコンピュータ（パソコン）やゲーム機に組み込むことによって構成される無線端末、を利用することにより、無線ケーブルモデム２０を介して、複数の無線端末１２，１４，１６…をインターネットに接続できる。

【００３９】つまり、無線ケーブルモデム２０は、無線ＬＡＮの一般的な仕様である「ＩＥＥＥ８０２．１１ｂ」に準拠したプロトコルで複数の無線端末１２，１４，１６…と無線通信を行うことで、これら各無線端末１２，１４，１６…とセンタ装置２内のＩＳＰ用の通信装置との間のデータ通信を中継する無線中継装置であり、各無線端末１２，１４，１６…は、この無線ケーブルモデム２０を介して、双方向ＣＡＴＶシステムが提供するＩＳＰとしてのサービス（つまりインターネット接続サービス）を享受できるのである。

【００４０】次に、このような中継機能を有する無線ケーブルモデム２０は、図２に例示するように、ＣＡＴＶ側送受信部３０と、デジタル変・復調部４０と、暗号処理部５０と、無線送受信部６０と、制御部７０と、ＥＥＰＲＯＭ等からなる不揮発性のメモリ８０と、を備える。

【００４１】ここで、ＣＡＴＶ側送受信部３０は、同軸コネクタＣＮを介して、同軸ケーブルからなる伝送線６の末端部に接続され、伝送線６を介して、センタ装置２内の通信装置との間で双方向通信を行うためのものであり、センタ装置２側から送信されてきた下り信号の中からデータ通信用の下り信号を抽出する選局部３４と、デジタル変・復調部４０から出力されたセンタ装置２への送信信号を所定周波数帯の上り信号に周波数変換する周波数変換部３６と、これら各部３４，３６と同軸コネクタＣＮとの間に設けられて、センタ装置２側から送信されてきた下り信号を選局部３４に入力し、周波数変換部３６から出力された上り信号を同軸コネクタＣＮ側に出力し、これら各信号の周り込みを防止する信号分離部３２と、から構成されている。

【００４２】また、デジタル変・復調部４０は、ＣＡＴＶ側送受信部３０（詳しくは選局部３４）から入力される下り信号からデジタルデータ（下りデータ）を復調し、暗号処理部５０に出力するデジタル復調部４２と、暗号処理部５０から入力されるセンタ装置２側への送信データ（上りデータ）を送信用の信号に変調し、ＣＡＴＶ側送受信部３０（詳しくは周波数変換部３６）に出力するデジタル変調部４４と、から構成されている。

【００４３】次に、暗号処理部５０は、制御部７０が実行する後述の端末登録処理によって上述したＷＥＰ用の暗号鍵が設定されているときに、外部の無線端末１２，１４，１６…との間で暗号化データを送受信できるようにするためのものであり、デジタル変・復調部４０（詳しくはデジタル復調部４２）から入力された下りデータを暗号鍵を用いて暗号化して無線送受信部６０に出力する暗号化部５２と、無線送受信部６０から入力される無線端末１２，１４，１６…からの受信データ（上りデータ）を暗号鍵を用いて復号化し、デジタル変・復調部４０（詳しくはデジタル変調部４４）に出力する復号化部５４と、から構成されている。

【００４４】また、無線送受信部６０は、アンテナＡＴを介して「ＩＥＥＥ８０２．１１ｂ」に準拠した２．４ＧＨｚ帯の無線電波を送受信することにより、無線端末１２，１４，１６…との間で無線通信を行うためのものであり、制御部７０は、無線端末１２，１４，１６…とセンタ装置２内の通信装置との間で行われるデータ通信を中継できるように上記各部３０，４０，５０，６０を制御するためのものである。

【００４５】そして、制御部７０は、ＣＰＵ，ＲＡＭ，ＲＯＭ等からなるマイクロコンピュータにて構成されており、上記中継のために行う上記各部３０，４０，５０，６０の制御に加えて、当該無線ケーブルモデム２０にてデータ通信の中継を行う無線端末を予め登録された無線端末１２，１４，１６，…に制限するための端末登録・監視処理を実行する。

【００４６】図３に示すように、この端末登録・監視処理では、まず、Ｓ１１０（Ｓはステップを表す）にて、ＣＡＴＶ側送受信部３０の選局部３４から出力される下り信号を監視し、続くＳ１２０にて、選局部３４から下り信号が出力されているか否かを判断することにより、無線ケーブルモデム２０が同軸コネクタＣＮを介して伝送線６に接続されているか否かを判断する。

【００４７】そして、無線ケーブルモデム２０が伝送線６に接続されていなければ、Ｓ１３０に移行して、当該無線ケーブルモデム２０を利用可能な無線端末を、無線端末側からの登録要求に応じて登録する端末登録処理を実行し、逆に、無線ケーブルモデム２０が伝送線６に接続されていれば、続くＳ１４０に移行して、Ｓ１３０の端末登録処理の実行により、当該無線ケーブルモデム２０を利用可能な無線端末が既に登録されているか否か（換言すれば無線端末の登録データが有るか否か）を判断する。

【００４８】尚、本実施例では、Ｓ１４０において、無線端末のＭＡＣアドレスが一つでも登録されているか否かによって、無線端末の登録データの有無を判断するようにされている。そして、Ｓ１４０にて、無線端末の登録データは存在しないと判断されると、Ｓ１６０にて全ての無線端末からのアクセスを禁止した後、当該処理を一旦終了し、逆に、Ｓ１４０にて、無線端末の登録データが有ると判断されると、続くＳ１５０に移行する。そして、Ｓ１５０では、当該無線ケーブルモデム２０にアクセスしてきた無線端末が、先に登録された無線端末であるかどうかを監視し、登録されている無線端末に対してのみデータ通信の中継を許可する、端末監視処理を実行する。

【００４９】次に、Ｓ１３０にて実行される端末登録処理は、図４に示す手順で実行される。図４に示すように、端末登録処理では、まずＳ２１０にて、無線送受信部６０が無線端末からの送信データ（上りデータ）を受信したか否かを判断することにより、無線端末から上りデータが送信されてくるのを待つ。そして、Ｓ２１０にて、無線送受信部６０が無線端末からの上りデータを受信したと判断すると、Ｓ２２０に移行して、暗号処理部５０から出力される上りデータを取り込み、この上りデータから、この上りデータの送信先アドレス（ＩＰアドレス）を取得する。

【００５０】尚、既述したように、暗号処理部５０は、暗号鍵が設定されている場合に、下りデータの暗号化及び上りデータの復号化を行うものであり、暗号鍵が設定されていなければ、これら各データをそのまま入出力することから、Ｓ２２０の処理実行時に、暗号鍵が設定されていなければ、制御部７０には、無線送受信部６０が受信した上りデータがそのまま取り込まれ、逆に、暗号鍵が設定されていれば、制御部７０には、復号化部５４にて復号化処理が施された上りデータが取り込まれる。

【００５１】次に、続くＳ２３０では、上りデータから取得した送信先アドレスが、当該制御部７０に予め設定されたＩＰアドレス（自己アドレス）であるか否か、換言すれば当該制御部７０に対する無線端末の登録要求が送信されてきたか否かを判断する。そして、Ｓ２３０にて、上りデータから取得した送信先アドレスが自己アドレスであると判断されると、Ｓ２４０に移行して、今回上りデータを送信してきた無線端末に端末登録用のＷｅｂページを表示させるための端末登録用データを生成し、これを暗号化部５２に出力することにより、暗号化部５２、及び、無線送受信部６０を介して、今回上りデータを送信してきた無線端末に端末登録用データを送信し、逆に、Ｓ２３０にて、上りデータから取得した送信先アドレスが自己アドレスではないと判断されると、そのまま当該処理を一旦終了する。

【００５２】ここで、Ｓ２４０の処理は、端末登録用のＷｅｂサーバとしての機能を実現する処理であり、この処理の実行により、上りデータを送信してきた無線端末には、図５に例示する端末登録用のＷｅｂページが表示される。図５に例示するように、このＷｅｂページは、無線ケーブルモデム２０の利用可能端末を特定するための識別情報であるＭＡＣアドレスを登録するためのＭＡＣアドレス登録領域７２と、無線ケーブルモデム２０が属する無線ネットワークの識別情報であるＳＳＩＤを登録するためのＳＳＩＤ登録領域７４と、無線ケーブルモデム２０が無線端末との間で無線通信を行う際に通信データを暗号化するＷＥＰを利用するか否か、及びＷＥＰを利用するのであれば、暗号鍵に６４ビットのデータを使うか１２８ビットのデータを使うかを指定するためのＷＥＰ選択領域７６と、ＷＥＰの利用を選択した際に、

暗号鍵の登録ページを要求するための登録ページ要求領域７８とから構成されている。

【００５３】このため、使用者は、無線端末に表示されたＷｅｂページを見ながら、ＭＡＣアドレス、ＳＳＩＤ、ＷＥＰ利用の有無を設定でき、ＷＥＰを利用する際には、暗号鍵の登録ページを要求して、その登録ページで、任意の暗号鍵を設定できる。

【００５４】尚、本実施例では、無線ケーブルモデム２０を利用するためには、少なくとも、無線端末のＭＡＣアドレスを登録することが必須とされており、ＳＳＩＤ及びＷＥＰについては、任意に設定できるようにされている。次に、Ｓ２４０にて、端末登録用のＷｅｂページ（端末登録用データ）を送信すると、今度は、Ｓ２５０に移行して、暗号処理部５０から出力される上りデータを監視することにより、Ｓ２４０で端末登録用データを送信した無線端末側から上述したＭＡＣアドレス、ＳＳＩＤ、ＷＥＰ等の登録情報（本発明の制限情報に相当する）が送信されてくるのを待ち、この登録情報を受信すると、続くＳ２６０にて、その受信した登録情報（受信情報）は正常か否かを判断する。そして、受信情報が正常であれば、Ｓ２７０に移行して、その受信情報をメモリ８０に格納することにより、無線ケーブルモデム２０を使用可能な無線端末を登録する。

【００５５】尚、無線端末からの登録情報の送信は、図５に示したＷｅｂページ上で、「適用」若しくは「取消」を指定することにより行われる。そして、Ｓ２７０では、Ｗｅｂページ上で「適用」が選択されることにより送信されてきた登録情報については、新規登録する情報として受け付け、Ｗｅｂページ上で「取消」が選択されることにより送信されてきた登録情報については、既に登録された情報の取消指令として受け付ける。

【００５６】また、Ｓ２７０において、無線端末から送信されてきた登録情報の内、ＭＡＣアドレス及びＳＳＩＤについては、無線ケーブルモデム２０を利用可能な無線端末を特定するための情報としてそのままメモリ８０に記憶するが、ＷＥＰ利用の有無及び利用する際の暗号鍵を表す情報については、暗号処理部５０を動作させるのに必要な情報であるので、メモリ８０に記憶するだけでなく、暗号処理部５０の制御情報として、暗号処理部５０にも設定する。

【００５７】そして、このようにＳ２７０にて、受信情報に従い当該無線ケーブルモデム２０を利用可能な無線端末を登録するか、或いは、Ｓ２６０にて、受信情報に異常があると判断すると、Ｓ２８０に移行して、受信情報の登録結果を無線端末側に送信し、当該処理を一旦終了する。

【００５８】次に、図６は、図３に示すＳ１５０にて実行される端末監視処理を表すフローチャートである。図６に示すように、端末監視処理では、まずＳ３１０にて、無線送受信部６０が無線端末からの送信データ（上

りデータ）を受信したか否かを判断することにより、無線端末から上りデータが送信されてくるのを待つ。そして、Ｓ３１０にて、無線送受信部６０が無線端末からの上りデータを受信したと判断すると、Ｓ３２０に移行して、暗号処理部５０から出力される上りデータを取り込み、この上りデータから端末識別情報を取得する。この端末識別情報は、基本的には、無線端末のＭＡＣアドレスであるが、上記端末登録処理によってメモリ８０に当該無線ケーブルモデム２０が属する無線ネットワークの識別情報であるＳＳＩＤが登録されていれば、上りデータからＳＳＩＤも取得する。

【００５９】そして、続くＳ３３０では、上りデータから取得した無線端末の識別情報であるＭＡＣアドレスがメモリ８０に登録されているか否かを判断すると共に、メモリ８０にＳＳＩＤが登録されていれば、上りデータから取得したＳＳＩＤがその登録されたＳＳＩＤと一致するか否かを判断することにより、今回上りデータを送信してきた（換言すれば当該無線ケーブルモデム２０にアクセスしてきた）無線端末は、当該無線ケーブルモデム２０を利用可能な無線端末として登録されているか否かを判断する。

【００６０】そして、Ｓ３３０にて、無線端末が登録済みであると判断されると、Ｓ３４０にて、その無線端末から当該無線ケーブルモデム２０へのアクセスを許可して、当該処理を一旦終了し、逆に、Ｓ３３０にて、無線端末が登録されていないと判断されると、Ｓ３５０にて、その無線端末から当該無線ケーブルモデム２０へのアクセスを禁止して、当該処理を一旦終了する。

【００６１】尚、上記端末登録処理により当該無線ケーブルモデム２０へのアクセスを制限する制限情報としてＷＥＰが設定されている場合には、暗号処理部５０が、登録された暗号鍵を使って上りデータの復号化を行うことから、上りデータを送信してきた無線端末が、同じ暗号鍵を使って上りデータを暗号化していなければ、暗号処理部５０で上りデータを復元できない。従って、当該無線ケーブルモデム２０へのアクセスを制限する制限情報としてＷＥＰが設定されている場合、無線ケーブルモデム２０と同じＷＥＰ設定がなされていない無線端末については、上りデータから端末識別情報を取得することができず、アクセスが禁止されることになる。

【００６２】以上説明したように、本実施例の双方向ＣＡＴＶシステムにおいては、加入者住宅１０に、加入者側の複数の無線端末１２，１４，１６…との間で無線通信を行うことにより、無線端末１２，１４，１６…とセンタ装置２内の通信装置との間のデータ通信を中継する無線ケーブルモデム２０が設置されている。

【００６３】そして、この無線ケーブルモデム２０は、データ通信の中継を行う無線端末を制限するために、当該無線ケーブルモデム２０を利用可能な無線端末のＭＡＣアドレスを予め登録しておき、ＭＡＣアドレスが登録されていない無線端末については、データ通信の中継を禁止し、しかも、無線端末のＭＡＣアドレスが登録されていない場合には（Ｓ１４０：ＮＯ）、データ通信の中継動作を実行しないようにされている。このため、本実施例の無線ケーブルモデム２０を用いれば、ＭＡＣアドレスが登録されていない無線端末からセンタ装置２への不正アクセスを確実に防止できる。

【００６４】一方、本実施例の無線ケーブルモデム２０では、上記制限情報を登録するための端末登録処理を、無線ケーブルモデム２０が伝送線６から外されているときに限って実行するようにされており、無線ケーブルモデム２０が伝送線６に接続される通常時には、当該無線ケーブルモデム２０を利用可能な無線端末を登録できないようになっている。このため、無線ケーブルモデム２０を不正使用するために、第三者が自分の無線端末のＭＡＣアドレスを登録できる機会は殆どなく、これによっても、第三者の無線端末からセンタ装置２への不正アクセスを防止できる。

【００６５】また、特に、本実施例の無線ケーブルモデム２０は、データ通信の中継を行う無線端末を制限するための制限情報として、ＭＡＣアドレス以外にも、ＳＳＩＤやＷＥＰ用の暗号鍵を任意に登録できるようにされているため、これらを登録することにより、第三者の無線端末からセンタ装置２への不正アクセスをより確実に防止できる。

【００６６】そして、本実施例の無線ケーブルモデム２０によれば、双方向ＣＡＴＶシステムの加入者が、無線ケーブルモデム２０を使用した無線ＬＡＮを自宅で構築しても、第三者による不正アクセスを確実に防止できることから、加入者以外の者が無線端末を使ってセンタ装置２へ不正アクセスすることによって、正規の加入者が不利益を被るのを防止できる。

【００６７】よって、本実施例の無線ケーブルモデム２０を利用すれば、インターネット接続サービス等を行う双方向ＣＡＴＶシステムの信頼性を向上し、加入者にとって安心して利用できる双方向ＣＡＴＶシステムを実現できることになる。尚、本実施例においては、図３に示すＳ１１０～Ｓ１３０の一連の処理が、本発明の制限情報登録手段として機能し、Ｓ１４０及びＳ１５０の一連の処理が、本発明の無線端末制限手段として機能する。また、暗号処理部５０は、本発明（特に請求項５）の暗号処理手段に相当し、不揮発性のメモリ８０は、本発明の記憶手段に相当する。そして、本実施例において、記憶手段を不揮発性のメモリ８０にて構成しているのは、無線ケーブルモデム２０への電源供給を遮断した際に、一旦登録した制限情報が消失するのを防止するためである。

【００６８】以上、本発明の一実施例について説明したが、本発明は、上記実施例に限定されるものではなく、種々の態様を採ることができる。例えば、上記実施例で

は、データ通信の中継を行う無線端末を制限するための制限情報を登録する端末登録処理を、無線ケーブルモデム２０が伝送線６から外されているときに限って実行するように構成したが、例えば、この端末登録処理は、使用者が無線ケーブルモデム２０に設けられた登録スイッチ（ＳＷ）を手動でオンした際に、実行するようにしてもよい。そして、この場合、端末登録・監視処理としては、例えば図７に示す手順で実行するようにすればよい。

【００６９】即ち、図７に示す端末登録・監視処理では、まず、Ｓ４１０にて、無線送受信部６０が無線端末からの送信データ（上りデータ）を受信したか否かを判断することにより、無線端末から上りデータが送信されてくるのを待つ。そして、Ｓ４１０にて、無線送受信部６０が無線端末からの上りデータを受信したと判断すると、Ｓ４２０に移行して、暗号処理部５０から出力される上りデータを取り込み、この上りデータから、この上りデータの送信先アドレス（ＩＰアドレス）を取得する。

【００７０】また、続くＳ４３０では、上りデータから取得した送信先アドレスが、当該制御部７０に予め設定されたＩＰアドレス（自己アドレス）であるか否かを判断し、上りデータから取得した送信先アドレスが自己アドレスであれば、Ｓ４４０にて、登録ＳＷがオンされているか否かを判断する。

【００７１】そして、登録ＳＷがオンされていれば、使用者により無線端末の登録が許可されていると判断して、Ｓ１３０′にて端末登録処理を実行した後、当該処理を一旦終了し、逆に、登録ＳＷがオンされていなければ（換言すれば、無線端末の登録が許可されていなければ）、当該処理を一旦終了する。尚、Ｓ１３０′の端末登録処理では、図４に示したＳ２１０～Ｓ２３０の処理を実行する必要はないので、Ｓ２４０～Ｓ２８０の処理が実行される。

【００７２】一方、Ｓ４３０にて、上りデータから取得した送信先アドレスが自己アドレスではないと判断された場合には、Ｓ１４０に移行して、メモリ８０内に無線端末の登録データ（ＭＡＣアドレス）が有るか否かを判断し、Ｓ１４０にて、メモリ８０内に無線端末の登録データは存在しないと判断されると、当該処理を一旦終了し、逆に、Ｓ１４０にて、無線端末の登録データが有ると判断されると、続くＳ１５０′に移行して、端末監視処理を実行する。尚、Ｓ１５０′の端末監視処理では、図６に示したＳ３１０の判定処理を実行する必要はないので、Ｓ３２０～Ｓ３５０の処理が実行される。

【００７３】このように、図７に示した端末登録・監視処理では、上りデータから取得した送信先アドレスが自己アドレスであり、無線端末からその登録要求を受けた際に、登録ＳＷがオンされているか否か、つまり、使用者により無線端末の登録が許可されているか否かを判断し、無線端末の登録が許可されているときにだけ、Ｓ１３０′の端末登録処理を実行するようにしている。

【００７４】そして、端末登録・監視処理を、このように実行するようにしても、使用者が登録ＳＷをオフするのを忘れなければ、第三者が自分の無線端末のＭＡＣアドレスを無線ケーブルモデム２０に登録できる機会は殆どなく、上記実施例と同様の効果を得ることができる。

【００７５】一方、上記実施例では、Ｓ１４０の判定処理にて、メモリ８０にＭＡＣアドレスが登録されていないと判断されると、Ｓ１６０にて全ての無線端末からのアクセスを禁止するものとして説明したが、Ｓ１６０の処理に代えて、図８に示す処理（Ｓ１６０′）を実行するようにしてもよい。

【００７６】即ち、この処理（Ｓ１６０′）では、Ｓ１４０の判定処理にて否定判断されると、上りデータから無線端末のＭＡＣアドレスを取得し（Ｓ５１０）、その取得したＭＡＣアドレスを構成しているベンダーＩＤが、当該無線ケーブルモデム２０に付与されたＭＡＣアドレスのベンダーＩＤと一致するか否かを判断して（Ｓ５２０）、ベンダーＩＤが一致している場合には、その無線端末からのアクセスを許可し（Ｓ５３０）、ベンダーＩＤが一致していなければ、その無線端末からのアクセスを禁止する（Ｓ５４０）。

【００７７】そして、このようにすれば、無線ケーブルモデム２０の所有者は、無線ケーブルモデム２０を購入する際、これとベンダーＩＤが同じ無線端末（若しくはＮＩＣ）を購入すれば、これらをそのまま使って、センタ装置２内の通信装置とデータ通信を行うことができるようになり、無線ケーブルモデム２０の使い勝手を向上できる。

【００７８】尚、この場合、無線ケーブルモデム２０に付与されたＭＡＣアドレスと同じベンダーＩＤのＭＡＣアドレスを有する無線端末については、何ら制限を受けることなく、無線ケーブルモデム２０を利用できることになるが、無線ケーブルモデム２０を不正に利用しようとする第三者は、この無線ケーブルモデム２０と同じベンダーＩＤの無線端末を準備しなければならないため、第三者による無線ケーブルモデム２０の不正使用を防止できる。

【００７９】また次に、上記実施例では、本発明の無線中継装置を双方向ＣＡＴＶシステムで用いられる無線ケーブルモデム２０に適用した場合について説明したが、本発明の無線中継装置は、無線端末から有線ＬＡＮに接続するのに用いられる無線ＬＡＮ用の基地局等にも適用できるのは、いうまでもない。

【図面の簡単な説明】

【図１】　実施例の双方向ＣＡＴＶシステムの概略構成図である。

【図２】　実施例の無線ケーブルモデムの構成を表すブロック図である。

17

【図３】　実施例の無線ケーブルモデムで実行される端末登録・監視処理を表すフローチャートである。

【図４】　図３のＳ１３０にて実行される端末登録処理を表すフローチャートである。

【図５】　図４の端末登録処理で加入者側の無線端末に提供されるＷｅｂページの一例を表す説明図である。

【図６】　図３のＳ１５０にて実行される端末監視処理を表すフローチャートである。

【図７】　端末登録・監視処理の他の実施例を表すフローチャートである。

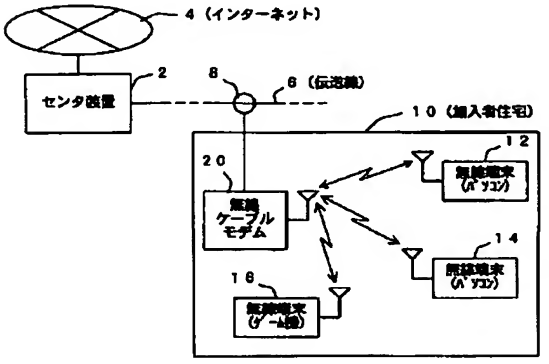
18

【図８】　図３に示した端末登録・監視処理の一部変形例を表すフローチャートである。

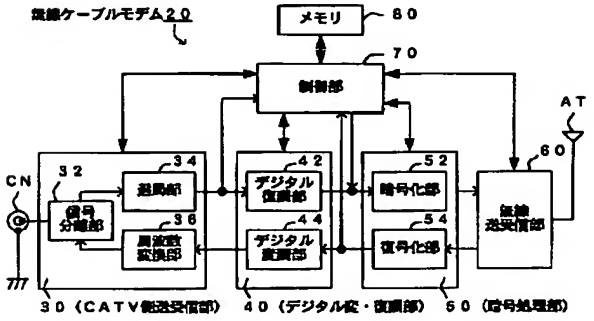
【符号の説明】

２…センタ装置、４…インターネット、６…伝送線、８…タップオフ、１０…加入者住宅、１２，１４，１６…無線端末、２０…無線ケーブルモデム、３０…ＣＡＴＶ側送受信部、４０…デジタル変・復調部、５０…暗号処理部、６０…無線送受信部、７０…制御部、８０…メモリ。

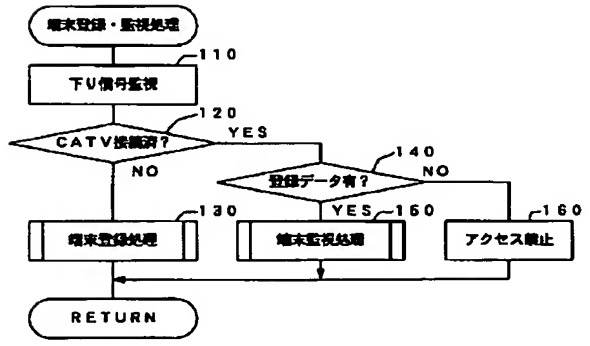
【図１】



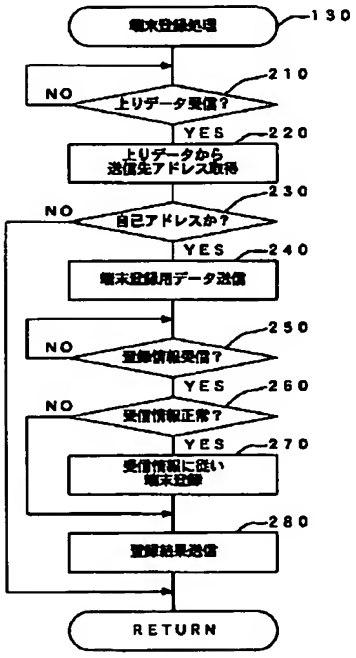
【図２】



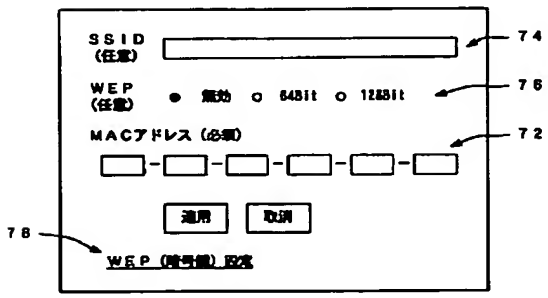
【図３】



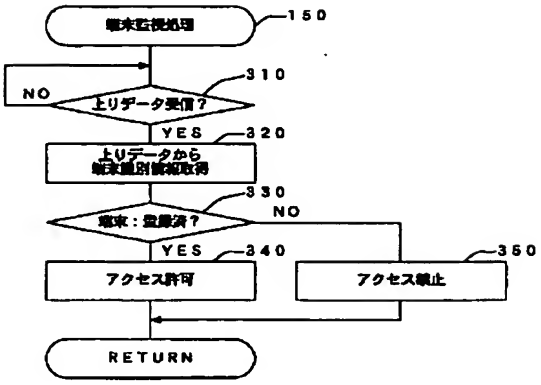
【図４】



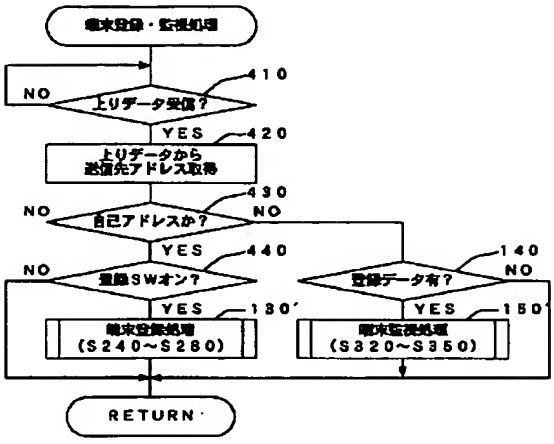
【図５】



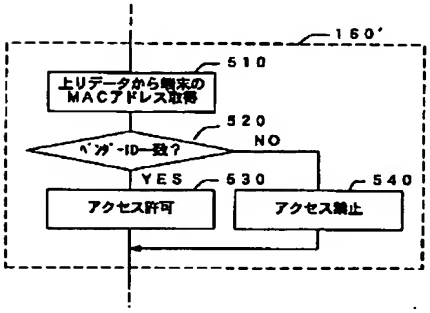
【図６】



【図７】



【図８】



フロントページの続き

Ｆターム(参考) 5K033 AA08 BA07 DA05 DA17 DB19
5K067 AA35 BB21 DD13 EE02 EE06
HH22 HH23
5K072 AA28 BB02 BB13 CC34 EE03
GG14